

Purpose

This policy ensures the safety and wellbeing of customers in Access4u's (we, our, us) care when using digital devices and engaging with online content. It outlines our key principles and best practice guidelines to promote a safe online environment and protect our customers from potential online risks and threats.

Scope

Compliance with this policy is mandatory for all employees involved in supporting our customers. This policy applies to customers who we have a duty of care for when they use online services, including websites, applications, communication tools, and any digital platforms.

Responsibilities and delegations

This policy applies to	Governing Body. Staff and Volunteers
Specific responsibilities	The Board – Responsible for ensuring effective governance mechanisms are in place. The CEO and Managers – Responsible for monitoring and ensuring adherence to Policy and related procedures. Ensure due diligence and take reasonable steps to ensure Access4u are meeting their obligations. Ensure objectives of the policy are achieved. Staff – Responsible for adherence to this and related policies, procedures and forms that support this policy.
Policy approval	CEO

Policy context – this policy relates to:

Standards	• Family and Community Services Act 1972 • National Disability Insurance Scheme Quality and Safeguarding Framework • National Standards for Out-of-Home care (NOOHCS) • The Office of the Guardian for Children and Young People - Charter of Rights
Legislation	• Children and Young People (Safety) (Transitional Provisions) Regulations 2017 • Children and Young People (Safety) Act 2017 (SA) • Children's Protection Law Reform (Transitional Arrangements and Related Amendments) Act 2017 • Criminal Law Consolidation Act 1935 (SA) • Disability Discrimination Act (DDA) 1992 • National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018

	• National Disability Insurance Scheme Act 2013 • National Principles for Child Safe Organisations • Online Safety Act 2021 (Cth) • Privacy 1988 (Cth) • Summary Offences Act 1953 (SA), • The Disability Act 2006 • The Disability Services Act SA 1993
Contractual obligations	• Government of SA, DCP Contract Management Framework • NDIS Code of Conduct
Organisation policies and procedures	• Supported decision making and consent policy • Code of conduct policy • Zero tolerance policy • Human rights policy • Duty of care and dignity of risk policy • Child safe environments policy • Child abuse report line (CARL) procedure • Customer Safeguarding policy • Privacy policy • Incident management policy
Forms, record keeping, other documents	

Policy Statement

The internet can be an excellent tool. It provides easy access to a world of information and can help people communicate and socialise with others. But the internet also has risks

- eSafety research on youth, kids and digital dangers¹, reports that one in four young people have been contacted by someone they don't know online and 50% of young people with a disability have talked to someone they don't know online.
- eSafety's social cohesion research² (respondents targeted to 12 to 17 year old Australian's) showed
 - 25% had been targets of bullying or hurtful comments online
 - 53% had seen or heard hateful comments about cultural or religious groups online
 - 37% Aboriginal and Torres Strait Islanders had been targets of harmful content online
 - 26% LGBTQIA+ had been targets of harmful content online

¹ <https://www.esafety.gov.au/...State of play - youth kids and digital dangers>

² <https://www.esafety.gov.au/...online-hate-bullying-violence>

- eSafety reports
 - Young people with a disability may be more likely to have contact with strangers online.
 - Culturally and linguistically diverse (CALD) young people are less likely to report negative online experiences.
 - LGBTQIA+ young people may be more likely to experience online abuse and hate speech.
 - Young people in out-of-home care may be more vulnerable to grooming.

The Online Safety Act 2021 (Cth) makes online service providers more accountable for the online safety of the people who use their service. This Act gives the eSafety Commissioner substantial powers to protect all Australians across most online platforms and forums where people can experience harm. Go to <https://www.esafety.gov.au/> for more information on the eSafety Commissioner.

There may be significant reputational, personal and legal risks associated with unsafe online behaviour. Without appropriate education, our customers may be victims of or guilty of a crime, such as image-based abuse (when someone shares or threatens to share an intimate image or video without consent).

Legislation that is relevant for our customers and employees include:

Criminal Code Act 1995 (Cth), where a child aged 10 years or more may be found criminally responsible for an offence if they knew their conduct was wrong.

Summary Offences Act 1953 (SA), where it is an offence to distribute invasive images of another person without their consent.

Child and Young Person (Safety) Act 2017 (SA), where the failure to report suspicion that a child or young person may be at risk is an offence.

Criminal Consolidation Act 1935 (SA), where it is an offence to not protect children from sexual abuse and not report any suspected child sexual abuse.

We are committed to creating a safe online environment for our customers. Through implementation of this policy, we aim to empower our customers to make responsible and informed choices when navigating the digital world whilst minimising potential risks and threats.

Key principles

Protection

- We are committed to protecting our customers from online threats, including cyberbullying, inappropriate content, and contact with potentially harmful individuals.
- Refer to our Code of conduct, Zero tolerance and Human rights policies for more information.

Education

- We will facilitate access to education and resources to our customers to enhance their understanding of online safety, responsible digital citizenship, and potential risks.
- We will ensure online safety education and resources are accessible, culturally safe and relevant to our customers with consideration of their individual needs and preferences.

- We aim to empower customers to make informed decisions and take responsibility for their online actions. Refer to our Duty of care and dignity of risk policy for more information.

Monitoring and reporting

- We will monitor online activities to ensure compliance with this policy and promptly report any suspicious or concerning online behaviour to appropriate authorities.

Privacy and consent

- We will respect the privacy and confidentiality of our customers' online activities.
- We will respect the privacy and consent of our customers when collecting and using their online data, ensuring compliance with applicable data protection laws.
- Refer to our Privacy policy and Consent procedure.

Support and intervention

- We will offer support and intervention when necessary to address online safety issues and provide guidance on appropriate responses.
- We will establish a confidential mechanism for customers to report online safety concerns or incidents, ensuring that they feel safe seeking assistance.
- Customers who experience online safety issues will be offered appropriate support and intervention, which may include counselling or referrals to external resources.

Guidelines

We acknowledge that no single strategy is 100% effective at keeping our customers safe online. Through combining a number of different strategies and approaches we will ensure our customers are as safe as possible with the following controls in place.

Access control

- We will implement appropriate access controls to restrict access to offensive, inappropriate, unsuitable and illegal content and services.
- We have implemented a standard approach across all our sites for network access to reduce cyber security risks. This includes
 - a centralised firewall performing internet traffic monitoring and scanning
 - a web filter that is configured to block access to websites that are unacceptable to be accessed under our policies
 - use of SafeSearch which is designed to filter out pages that contain images or videos that contain body images or sexual content. It also is designed to filter pages with links, pop-ups, or ads that display or point to explicit content.
 - image filtering is enabled for Google and Bing which filters images with a creative commons license.

- a custom URL blocklist of alternative search engines so that other search engines cannot be used to access inappropriate material.
 - setting the restriction level for YouTube Restricted Mode to moderate.
- All of our sites, including residential homes, have a Wi-Fi network that our customers can access as 'guest' for educational and recreational purposes. Portable pre-paid modems or dongles are not recommended as they do not provide adequate security and monitoring.
- Where possible, we encourage children and young people in our residential services to access online services in common areas of the home. It is recommended they do not have access to online services for prolonged periods of time in their bedrooms.
- Denying our customers access to the Wi-Fi may be considered a restrictive practice. It is important to consider access and time limitations to the Wi-Fi on a case-by-case basis, paying attention to the quality of activity and the length of time customers spend online, eg online time may be extended for customers requiring access for homework or other educational activities. We will ensure our customers develop a range of offline skills and interests.

Devices and online accounts

- Due to the nature of devices, and content that may be stored on them, it is preferable that devices are new. For DCP customers, any devices must be approved for reimbursement from DCP prior to purchase. Any second-hand device must be thoroughly checked and approved prior to use by our IT Department, including hard drives and USBs that may contain multimedia.
- When assisting customers to install apps or create accounts, developer's recommendations for minimum age must be adhered to.
- We will promote the use of strong, unique passwords and educate our customers on the importance of keeping their login credentials confidential.

Education

- Communication about online safety and cyber safety is a key to promoting safe and positive online behaviour. This includes conversations around safety and confidentiality, acceptable online behaviours, legal accountability, restrictions to content and strategies to navigate factual versus false information on the internet. The online safety agreement is a useful tool for this purpose (refer below).
- There are a range of interactive online training modules and sites which actively promote safe internet use and educate about the potential dangers of using the internet, and how to safely manage an online presence. These include (but are not limited to)
 - eSafety Commissioner: <https://www.esafety.gov.au/educators/video-library>
 - Interaction services free online safety training: <https://interactionservices.org/online-safety/>
 - Think u know: <https://www.thinkuknow.org.au/resources-tab/parents-and-carers>
- We will facilitate education for our customers about the potential risks of online relationships and the

importance of not sharing personal information with strangers.

- Internet safety cards that provide cues to support online safety, appropriate behaviours and safe online relationship development <https://www.secca.org.au/resources/internet-safety-cards/>
- We will facilitate education for our customers about cyberbullying, its effects, and how to report incidents. We will take appropriate action against cyberbullies within our programs. Refer to <https://www.esafety.gov.au/key-topics/cyberbullying> for more information.
- We will facilitate access to programs and resources to enhance digital literacy skills for our customers.
- Encourage open conversations about technology and online behaviour and use opportunities for 'incidental education'.

Safety breaches

- We will ensure our customers know who they can go to, and what to do if something happens that makes them feel unsafe or uncomfortable when they are online.
- If our customers are found to be accessing inappropriate material or show unsafe online behaviours, we will use this opportunity to reflect on their online safety agreement and support access to online safety training and aid in conversations around safety.
- We will provide a clear and confidential process for reporting online safety incidents with external sources, ensuring our customers feel safe reporting concerns and know that nothing is ever so bad that they cannot tell a trusted person.
- We will monitor and assess any unsafe online behaviour and consider if there are any legal implications that may require intervention by external agencies.
- We support our customers to report any complaint about cyberbullying, adult cyber abuse, image-based abuse (sharing, or threatening to share, intimate images without the consent of the person shown) or illegal and restricted online content to eSafety <https://www.esafety.gov.au/report/forms>.
- We will report any inappropriate, harmful or criminal activities that have occurred to children online to the Child Abuse Report Line (CARL) on 13 14 78 and to the Australian Centre to Counter Child Exploitation (ACCCE) <https://www.accce.gov.au/report>.
- If we feel our customer is in immediate danger, we will call SAPOL on 000 (triple zero).
- Refer to our Child safe environments policy, Adult Safeguarding policy, Incident management policy, and Child abuse report line (CARL) procedure.